HONG KONG MONETARY AUTHORITY
香港金融管理局

儲值支付工具持牌人
監管的應用說明

2022 年 3 月

內容

1. 引言

1.1. 香港金融管理局(金管局)發出的《儲值支付工具持牌人監管指引》(《指引》)列載金管局在評核儲值支付工具持牌人是否適當人選時所採用的高層次監管原則。為使持牌人更了解應用《指引》所載原則的標準，金管局會在有需要時發出《儲值支付工具持牌人監管的應用說明》(《應用說明》)，就《指引》的特定章節提供附加指導。

1.2. 持牌人應視《應用說明》為在典型的情況下可如何符合某項原則性規定的具體說明。 持牌人應透徹理解有關指導，並在考慮其具體情況後，適當調整其管控制度，以遵守《指引》的規定。《應用說明》應與《指引》的有關章節及金管局不時發出的有關《常見問題》一併閱讀。

1.3. 為免引起疑問，有關儲值支付工具持牌人的監管規定載於《支付系統及儲值支付工具條例》(《支付條例》)及《指引》。雖然《應用說明》可協助持牌人更充分了解如何遵從有關規定，但不會凌駕或取代該等文件內的任何條文。

1.4. 此《應用說明》只列載有發出附加指導的《指引》的特定章節。金管局日後可能會在有需要時修改現有附加指導，或就《指引》的另一些章節增發附加指導，並以修訂《應用說明》的形式發佈。由於資源所限，輕重緩急會基於持牌人提出的意見及其實際經驗而定。

2. 主要業務及財政資源

金管局會在有需要時發出附加指導。

3. 企業管治

《指引》第 3.2 條 － 企業管治

《指引》3.2.1	*持牌人須有穩健的管治安排，以能作出有效決策，以及妥善管理及管控其業務和運作所產生的風險。有關安排應包括清晰的組織架構，並附有清楚界定、具透明度及貫徹的職責分配，並應有有關決策程序、匯報渠道、內部匯報及通訊程序的清晰文件紀錄。*
附加指導	(a) 作為穩健的管治安排的一部分，持牌人應制定操守準則，列明管理層及員工應有的誠信和操守標準，以及有關其行政總裁、董事及經理須按照《支付條例》符合適當人選的相關條件。持牌人亦應設有周全制度以落實執行其操守準則。 (b) 持牌人應對有關管治安排及風險管理與內部管控制度是否周全及有效，定期進行風險為本的獨立評估。而持牌人應至少每年一次對其運作涉及的主要風險環節進行自我評估，以決定上述該獨立評估的範圍及次數。

《指引》3.2.2	*持牌人的董事局應對持牌人的儲值支付工具的穩健運作與審慎管理負有最終責任。因此，持牌人董事局的責任、組織、運作及組成必須清楚界定及以文件記錄。*
附加指導	(a) 持牌人的董事局一般應決定其結構、組成及職責範圍，但為確保儲值支付工具業務的穩健運作及得到審慎管理，董事局的職責一般包括但不限於以下各項： (i) 設定持牌人的目標、風險承受度及企業價值觀，以及批准達到該等目標的策略，使公司能維持於有關風險承受水平之內及秉持有關企業價值觀； (ii) 批准主要政策，以建立強而有力的風險管治及有效的管控制度，從而使持牌人透過採用穩健而審慎的做法，以安全及有效率的方式運作； (iii) 監督高級管理層員工的表現，以確保他們按照經批准的政策履行其職責，並在其獲授的權力範圍內履

行其職責；以及

(iv) 確保有效設立主要管控部門(包括但不限於業務操作及資訊科技風險管控、合規、內部審計及外部審計)，及其具充分獨立性，不受業務部門影響。

《指引》 3.2.3	*董事局應有足夠人數及適當的成員組合，以確保有充足的制衡及集體專門知識，以作出有效及客觀的決策。各機構董事局的規模及組成視乎持牌人的規模、複雜程度及其業務性質和範圍而有所不同。作為反映有充足制衡的一般基準，董事局通常應有三分之一的成員為獨立非執行董事。*

附加指導

(a) 若持牌人能向金管局證明並令金管局確信，基於其結構及情況，持牌人難以或無法嚴格遵守有關《指引》，金管局可考慮接受替代安排，而有關安排需具有相同效力，可確保董事局內有充足制衡及集體專門知識。

(b) 在考慮某人是否合資格及適合擔任(或繼續擔任) 獨立非執行董事時，持牌人應評估該人是否具備所必要的獨立性。舉例來說，相關評估因素包括：

(i) 該人在該持牌人或其股東控權人(按《支付條例》的定義)、集團公司或附屬公司的持股量或金融交易(如有)；

(ii) 該人最近曾否為該持牌人或其股東控權人(按《支付條例》的定義)、集團公司或附屬公司的僱員、主管人員或董事(獨立非執行董事除外)；

(iii) 該人與持牌人或其股東控權人(按《支付條例》的定義)、集團公司或附屬公司是否有任何重大業務關係，或從該持牌人或其股東控權人(按《支付條例》的定義)、集團公司或附屬公司收取任何大額補償，惟就擔任獨立非執行董事提供服務而收取的酬金除外；

(iv) 該人與持牌人或其股東控權人(按《支付條例》的定義)、集團公司或附屬公司是否有任何緊密關連；以及

(v) 該人是否有任何會引致利益衝突的角式。

(c) 持牌人應確保獨立非執行董事並非其主管人員之一，亦不

	會負責日常管理，包括但不限於參與其管理層級別的委員會。
《指引》 3.2.5	*董事局對持牌人的整體穩健情況負有最終責任，而委任能幹的管理層是確保業務穩健及有效管理的關鍵。董事局應與高級管理層團隊(高級管理層)合作，以達到上述目標，而高級管理層則向董事局負責。*
附加指導	(a) 正如《指引》第 3.2.2 段的附加指導所載，董事局在履行其職責時，可向高級管理層下放適當權力，但應設有有效安排，讓董事局可評核高級管理層的表現，並就未能令人滿意的表現向其問責。
《指引》 3.2.6	*高級管理層負責按照董事局設定的業務策略、政策、風險承受水平及轉授的權力，有效及審慎地管理持牌人的業務。*
附加指導	(a) 一般而言，除了別的以外，高級管理層應負責以下職責： (i) 提出業務計劃、政策、主要表現指標及風險限額的建議供董事局審議及批准； (ii) 制定穩健的管控制度，有關制度一般應涵蓋適當的職責劃分、清晰的責任分配及授權、充足的內部牽制及對帳、有效及適時的資訊科技系統及管理資訊系統、穩妥的員工招募、培訓及評核計劃，以及獨立的內部審計及合規部門；以及 (iii) 根據董事局批准的業務策略、風險承受度及政策，制定有效的風險管理制度，以管理持牌人的業務活動所引起的不同範疇的風險。

《指引》 第 3.3 條 － 高級人員及控權人須為適當人選

《指引》 3.3.2	***董事及行政總裁*** *鑑於董事及行政總裁負有領導責任，因此在評估某人是否該等崗位的適當人選時，會考慮其誠信及能力。一般而言，這會從其相關知識、經驗、判斷力及領導素質等方面作出考量。同時，亦會評估該等人士對相關儲值支付工具業務投入充足時間及*

關注的承諾及能力。視乎持牌人的業務規模及複雜程度而定，有關人士就這幾方面要求須達到的標準會有所分別。

附加指導

(a) 金管局在評核某人的誠信時，一般會審核是否有任何紀錄、事件或事宜會令人懷疑其誠實正直。雖然未能羅列所有相關情況，但在以下典型情況中，有關人士須向金管局證明並令其確信有關情況不會對該人的誠實及正直引起疑問：

(i) 該人曾被任何監管機構或專業團體對其採取紀律行動(如譴責、罰款及暫時吊銷牌照)；

(ii) 該人曾被判犯刑事罪行；

(iii) 該人為未解除破產債務的破產人、現正進行破產程序或有破產記錄；

(iv) 該人曾被法庭或其他主管當局裁定為犯欺詐、不誠實或失當行為；

(v) 有記錄顯示該人曾作為已清盤或無力償債的公司或業務的控權人、行政總裁、董事或經理；以及

(vi) 該人從事法例規定需要特定牌照、註冊或其他授權的業務或專業的權利被拒絕或限制。

(b) 金管局在評核某人的能力時，會考慮該人的行業經驗、管理經驗、學歷及專業資格、對儲值支付工具營運及產品的知識，以及監管知識。金管局亦會審核是否有任何可能會令人懷疑其能力或領導才能的紀錄、事件或事宜。雖然未能羅列所有相關情況，但在以下典型情況中，有關人士須向金管局證明並令其確信有關情況不會對該人的能力引起疑問：

(i) 該人曾因不稱職、疏忽或管理不善而被專業團體、業內組織或監管機構紀律懲處；

(ii) 該人曾因不稱職、疏忽或管理不善而從任何崗位或職位被撤職或被要求從任何崗位或職位辭職；

(iii) 該人為未解除破產債務的破產人、現正進行破產程

序或有破產記錄；

(iv) 有記錄顯示該人曾作為已清盤或無力償債的公司或業務的控權人、行政總裁、董事或經理；以及

(v) 該人從事法例規定需要特定牌照、註冊或其他授權的業務或專業的權利被拒絕或限制。

金管局在考慮有關個案時，會考慮到事件的性質與嚴重程度、有關人士在事件中的角色及責任，以及有關人士自事件發生以來所採取的行動及作出的改進等因素。金管局會要求有關人士解釋為何該等紀錄、事件或事宜並不反映其能力不足，或其後作出了甚麼行動以提升其能力。

《指引》3.3.3.1

控權人

在評估控權人是否適合人選時，主要考慮因素之一是控權人對有關計劃使用者及潛在使用者的利益的潛在影響。這一點需要按每宗個案本身的情況來衡量。一般的假定是控權人對持牌人的影響力越大，對控權人符合準則所要求的標準便會越高。控權人是否願意及有能力與其他控權人及管理層團隊合作，亦是主要考慮因素之一。

附加指導

(a) 在評核持牌人的控權人申請人的潛在影響力時所考慮的因素包括

(i) 相比其他現有股東控權人，申請人所建議的持股量；

(ii) 將會被提名代表申請人的董事數目；

(iii) 申請人尋求成為控權人的目的，例如維持持牌人的現狀或對持牌人的業務策略或組織架構作出重大改動；以及

(iv) 是否有任何書面協議或承諾，例如承諾不干預持牌人的業務策略。

《指引》3.3.4.1

經理

	在評估經理是否適合人選時，會應用就董事及行政總裁設定的相若原則，但會因應經理負責的具體業務或管控範疇作出評估。根據《支付條例》附表3第3(3)條，持牌人設有適當及周全的管控制度，以確保其每名經理均是擔任有關職位的適當人選。
附加指導	(a) 為確保持牌人的經理為適當人選而設立的適當及周全的管控制度一般具有以下特點： (i) 妥善及及時地識別所有符合《支付條例》所列載「經理」的定義的職位； (ii) 個別經理級職位的職責及所需技能、知識及經驗應清楚界定，並有最新的職位說明、組織架構圖及權力級別為證； (iii) 設有妥善的政策及程序甄選及委任經理，以及令持牌人確信有關候選人是擔任或將會擔任該職位的適當人選； (iv) 設有有效的制度，按照經理的表現對其作出評核、獎勵及紀律懲處，並定期評核其是否為適當人選； (v) 設有政策及程序，以調查經理違反規則及規例的情況或對經理的投訴，以及因應調查結果採取紀律行動； (vi) 經理級的空缺迅速得到填補，以及有清楚界定的安排應付暫時出現空缺的情況； (vii) 向經理提供充足培訓；以及 (viii) 內部審計部門定期檢討有關委任經理的管控制度。

《指引》 第 3.4 條 – 外判

《指引》 3.4.3	*持牌人外判其任何運作或功能時，應(a)妥善籌劃外判安排，包括進行全面的風險評估，以識別及評估涉及的所有風險；外判的安排應能確保所有已識別的重大風險(包括業務受干擾的風*

	險)在推出前已得到周全的管理；以及外判安排不會影響其內部管控的成效，或損害儲值支付工具使用者的利益；(b)妥善實施外判安排，包括對服務提供者進行適當的盡職審查；進行適當測試以確保所提供的服務完全符合所協定的效能標準；與服務供應商訂立適當的外判協議，清楚列明外判安排及相關的權利與義務；以及妥善轉移有關運作或功能，以確保順利過渡；以及(c)持續妥善管理外判安排，包括對外判的運作或功能進行適當的定期質量檢討，以確保所提供的服務繼續完全符合所協定的效能標準，發現的所有缺失都已妥為糾正；進行適當的定期風險評估，以確保在持續基礎上妥為識別、評估及周全管理所有重大風險；以及每隔一段適當時間檢討外判協議，以評估應否重新商討及更新有關協議，從而使其與當前市場標準一致，以及應對持牌人業務策略的轉變。
附加指導	(a) 一般而言，對服務提供者進行的適當盡職審查除考慮成本因素及服務質素外，應考慮到提供者的財政穩健情況、信譽、管理能力、技術能力、營運能力、應付持牌人長期需求的操作能力、對支付行業的認識，以及緊貼市場創新的能力。 (b) 一般而言，適當的外判協議應清楚列明(a)所提供的服務類別及水平，以及服務提供者的相關執行標準，包括就日常操作及系統問題的應變安排；(b) 服務提供者的合約義務及責任；(c)持牌人的權利及義務，包括持牌人應支付的有關費用及收費，以及持牌人在香港適時存取、檢索及保存準確及最新的記錄，以及如需要，向有關當局(包括金管局)提供有關記錄以供查閱的權利；以及(d)處理數據，例如儲存、備份、保護和保密、以及合約終止或屆滿時移除數據的安排等方面的管控措施。 (c) 一般而言，因外判安排以致業務受干擾的風險可透過應變安排予以處理。服務提供者本身的應變計劃通常會涵蓋有關日常運作及系統問題的應變安排。一般而言，持牌人應確保其充分了解其服務提供者的應變計劃，並考慮一旦外判服務因服務提供者的系統故障而中斷對其本身的應變計劃的影響[1]。如切實可行，持牌人及其服務提供者應定期

[1] 服務提供者可能會因無力償債或其他原因而未能繼續提供服務及支援。

測試該等應變計劃。

(d) 就境外外判而言，除上述的考慮因素外，外判安排一般應處理以下事宜：

(i) 境外外判對持牌人的風險狀況的影響；

(ii) 境外主管當局(如警察及稅務當局)取用使用者的資料的權利(如境外主管當局試圖取用其使用者的資料，持牌人應通知金管局)；

(iii) 通知客戶；

(iv) 外判後有關香港主管當局(包括金管局)取用使用者資料以作審查的權利；以及

(v) 規管外判協議的法律。

《指引》3.4.4	*持牌人應確保外判安排符合《個人資料(私隱)條例》(「《私隱條例》」)及個人資料私隱專員公署(「私隱公署」)不時發出的任何相關實務守則、指引及最佳做法。*
附加指導	(a) 一般而言，要確保合規，持牌人可透過制定有效措施，以確保服務提供者妥為遵守《私隱條例》下的所有適用法定及監管規定，尤其是按照《私隱條例》的規定向使用者發出通知或徵求使用者同意，並妥善保存有關紀錄。如有需要，持牌人應尋求法律意見。
《指引》3.4.5	*外判不應妨礙有關主管當局的審查人員及持牌人的內部及外聘核數師取用資料。持牌人應確保設有周全及有效的安排，以便利獲授權第三方(例如持牌人的內部核數師、外聘核數師/評估員及金管局)進行已宣布及未經宣布的現場及非現場審查。*
附加指導	(a) 一般而言，周全的安排包括在與服務提供者訂立的外判協議訂有一項條款，容許監管當局視察或檢討服務提供者涉及外判活動的運作及管控措施(包括有關當局(包括金管局)可不受限制地進入有關處所及系統，以及取用有關記錄及文件) ，並應就有關安排取得有關地區的主管當局(如有)的指明同意。

4. 一般風險管理及內部管控制度

金管局會在有需要時發出附加指導。

5. 資訊及會計系統

金管局會在有需要時發出附加指導。

6. 儲值金額及工具按金的管理

《指引》第 6.2 條 － 一般原則

《指引》 6.2.1	*持牌人應設立有效及穩健的制度，以保障及管理儲值金額及工具按金，從而確保所有資金都只撥作指明用途；屬於儲值支付工具使用者的資金得到保障，在任何情況下都不受儲值支付工具發行人的其他債權人提出的申索影響，亦不會受其運作及其他相關風險所影響。*
附加指導	(a) 本章接下來的部分就構成有效及穩健系統的元素提供指引。其中部分期望是與確保儲值金額及工具按金的法律明確性及運作安全有關。一般而言，持牌人應尋求外聘法律意見，以確保法律確定性，並委託外聘獨立人士進行審核，以確保運作穩健。有關期望包括持牌人對保障及管理儲值金額及工具按金的系統作出任何重大改變前，亦會尋求上述的外聘法律意見和委託外聘獨立人士進行審核。由於風險為本的方法會被採用，若持牌人能提供充分理據，其他方式的獨立核證可能會被考慮。 (b) 持牌人應至少每年一次對儲值金額及工具按金的保障和管理制度進行獨立檢討或審計，以確保其有效性及穩健性。 (c) 持牌人對保障及管理儲值金額及工具按金的系統作出任何重大改變前，應先諮詢金管局。

《指引》第 6.3 條 － 儲值金額及儲值支付工具按金的保障

《指引》 6.3.1	*持牌人應有有效的信託安排，以在持牌人一旦無力償債時，確保使用者對儲值金額及工具按金的法定權利及優先索償權。若持牌人能提供理據，有效的銀行擔保及/或保險保障可作為替代或補充安排。為免引起疑問，因儲值支付工具使用者選擇從其銀行帳戶或信用卡帳戶而非其儲值支付工具使用者帳戶直接扣帳而產生的在途資金會被視作從有關儲值支付工具使用者收到的儲值金額，並應受到同等程度的保障。*

附加指導

在各種有效的信託安排中，持牌人就其存於持牌銀行或金管局承認的外地銀行的獨立帳戶屬於儲值金額及工具按金的資產作出信託聲明，是可接受的做法。

(a) 持牌人應妥善指定該等獨立銀行帳戶作為持有在其信託安排下的儲值金額及工具按金之用。例如有關獨立銀行帳戶的相關詳細資料應載於(i)有關信託聲明中；(ii)有關信託聲明的附件；或(iii)按有關信託聲明所載安排及程序備存的記錄冊內。指定銀行帳戶的程序亦應由具備適當權力的單位(如董事局或行政總裁)批准，並備有審計追溯紀錄。

(b) 應支付予某儲值支付工具計劃的帳戶的所有款項(如帳戶增值)或應從某儲值支付工具計劃的帳戶收取的所有款項(如對商戶的付款)，包括在途資金，都應視作儲值金額，並賦予同等程度的保障。應支付予商戶的支付工具帳戶的款項，不論是否源自另一個支付工具使用者帳戶或自其銀行帳戶或其他卡帳戶直接扣帳，亦應被視作儲值金額，並賦予同等程度的保障。

《指引》6.3.2	*若情況所需，要向使用者退回儲值金額及工具按金，信託安排應包含妥當的法律地位及授權，以確保退款程序暢順及具效率。*

附加指導

在信託安排下，持牌人應設有退出計劃，而有關計劃一般應得到董事局層面的認可，並應包括：

(a) 會啟動向使用者退回儲值金額及工具按金的機制的特定情況清單(例如決定退出儲值支付工具業務、清盤)。如適用，應制定監察指標以確保在指明情況發生時能及時啟動退出計劃。

(b) 確保退款程序暢順及具效率的詳細步驟。金管局在評核退款程序是否具效率時會考慮的因素包括但不限於：向有關使用者發出通知、使用者預計可收到退款的時間、使用者為獲得退款而需要辦理的手續、以及出現無法退款情況的可能性(例如未能聯絡使用者)。

(c) 對有關程序的法律確定性及運作可行性的評核。

《指引》 6.3.3	*持牌人應確保在任何時間都有充足資金向所有儲值支付工具使用者退回儲值金額及工具按金，以及有充足額外資金支付在有需要時向所有使用者分派儲值金額及工具按金的所需費用。*
附加指導	(a) 持牌人應定期審慎估算有效進行其退出計劃中的退款程序(見6.3.2)所需的成本及工具按金(包括一旦退出儲值支付工具業務時應退還予使用者的任何在途資金)，而成本估算應考慮該計劃所列出的相關因素（包括使用者數目和儲值金額等）。持牌人應根據該估計成本設立有效程序，以確保在任何時間都預留充足的額外資金處理退款。例如在儲值金額及工具按金之上維持一筆額外/緩衝資金。持牌人應就如何釐定額外/緩衝資金制定周全的政策及程序，例如相關因素及公式(如適用)。此外，持牌人亦應制定周全的管控措施，以記錄該等額外/緩衝資金的釐定及維持，以及監察有關安排的成效與穩健程度。 (b) 若持有儲值金額及工具按金的帳戶所持有資產的款額低於分類帳系統所記錄的儲值金額及工具按金的款額，即出現短欠情況，持牌人應迅速向其高級管理層及金管局上報，不應延誤。一般而言，向金管局呈交的報告應涵蓋有關個案的成因及相關詳情、為糾正短欠情況所採取的行動等。
《指引》 6.3.5	*有關儲值支付工具計劃的儲值金額及工具按金的資產(包括現金及銀行存款)應與持牌人本身的資金及從其他業務活動收到的資金分隔獨立處理。*
附加指導	(a) 若持牌人運作超過一項儲值支付工具計劃，一般預期每項儲值支付工具計劃的儲值金額及工具按金會以分隔方式持有。
《指引》 6.3.6	*持牌人應有有效的內部管控措施及程序，以保障儲值金額及工具按金免受所有運作風險影響(包括盜竊、欺詐及挪用的風險)，而該等措施及程序應構成持牌人的整體穩健內部管控制度的重要部分。*

附加指導

(a) 為確保保障儲值金額及工具按金的管控制度的成效，持牌人通常須設有因應其經營模式、運作程序及系統設計的風險特性而特別制定的管控制度，有關制度一般應得到董事局層面的認可。以下列載的是一些通常會設立的內部管控措施：

(i) 職責劃分：前線業務部門、後勤運作部門及管控部門應保持獨立，並適當分隔，以確保有充足的制衡。同時上述每個部門都應設有清晰的從屬關係，並通常應由職級相若的高級管理人員擔任主管，以確保獨立性。

(ii) 管控政策及程序：管控政策及程序應清晰，可以執行，並有明確的準則、觸發因素及/或指標。持牌人應定期檢討其管控政策及程序，而檢討應考慮到經營模式、業務運作規模、運作程序、技術應用、有關各方的意見，以及規則與規例的任何改變。

(iii) 識別及緩減風險：持牌人應進行嚴謹的程序，以識別所有可能會引致盜竊、欺詐、挪用或任何其他形式的運作損失的風險及漏洞。持牌人應在其管控政策及程序中加入可有效應對所識別的風險及漏洞的具體管控措施。

(iv) 授權管控：一般預期有效的管控制度設有：(a)嚴謹的授權程序，以確保所有主要運作都經適當授權，例如銀行帳戶的運作、認可商戶名單的更改等；(b)及時偵測及防範未經授權的活動；(c)認真跟進或調查顯示試圖進行未經授權活動的情況的事件。

(v) 內部管控程序：雖然個別持牌人的詳細內部管控程序或有很大分別，但應就所有主要業務、運作程序及重要的系統輸入或更新步驟設有典型的內部管控方法，包括輸入及核對安排及帳目的定期對帳。持牌人應確保負責監察觸發事件的人員熟識相關業務操作。持牌人亦應制定周全的管控制度，確保負責若干職能(如匯報職能)的外部各方(如託

管人)全面了解其責任。

(b) 在不限制持牌人運用更先進及有效的管控措施的情況下，下文列出典型的運作模式應具備的主要管控元素：

(i) 有經過妥善測試及嚴謹實施的程序，以確保持牌人的儲值金額及工具按金有及時與準確的資金進出紀錄，而就系統紀錄與實際的儲值金額及工具按金(例如持有儲值金額及工具按金的專用銀行帳戶結餘)作定期對帳。同時，每日應定時提供定期管理資訊系統的報告。持牌人應有安排讓金管局可有效地查閱管理資訊系統的報告，以進行隨機非現場監管查核。對帳過程中發現的特殊情況應及時在內部上報及調查。如屬重大特殊情況(將由金管局與持牌人議定)，應盡快通知金管局。

(ii) 有經過妥善測試及嚴謹實施的程序以有效篩查支付指示，確保只向獲授權的收款人付款。預期持牌人的系統設計能及早偵測到對未經授權的收款人的支付指示，從而能暫停執行有關指示，以待額外覆核。

(iii) 為儲值金額及工具按金的安全及充足程度提供進一步保障的額外措施。可能的額外保障形式包括由獨立第三方(例如持牌銀行或金管局承認的外地銀行)的有效支付管控、保險保障或由銀行或其他信譽良好的人士(例如財政健全的集團公司)提供的擔保。為免引起疑問，以上所列僅屬可供選擇的方案，持牌人可提出其他可提供進一步保障的有效方法予金管局考慮。需要額外保障的程度視乎多項因素而定，包括金管局對持牌人有關儲值金額保障的內部管控措施的成效及穩健程度的評估、儲值金額及工具按金的規模及變動情況，以及持牌人的財力等。持牌人應在金管局的持續監管過程中與金管局討論及議定詳細安排。

《指引》 6.4.1	*儲值支付工具計劃的儲值金額及工具按金的管理應以流動性管理為主要目的，以確保經常有充足資金應付贖回。持牌人應就其持有的儲值金額及工具按金的相關資產，設有有效及與其儲值支付工具計劃的運作模式相符的流動性管理政策、指引及管控措施。*
附加指導	(a) 就可能出現的不同情況，例如使用者能在帳戶增值後立即運用或提取其儲值支付工具帳戶的資金，即使與帳戶增值相關的有關資金要待一段時間(可能幾個工作天)後才會存入持有儲值金額的持牌人指定帳戶，持牌人將須承受更高的流動性要求。該等流動性要求可能會因為不同的外部環境，例如有一些可能推動使用者運用特定增值渠道及/或特定儲值支付工具服務/功能的活動，而出現迅速和動態的變化。持牌人應制定有效機制，以監察及評估其流動性要求，並及時採取穩健措施，以管理及應對其流動性要求。 (b) 在評估管控措施的成效時，金管局計及持牌人在管理其流動性要求方面的專門知識及往績。
《指引》 6.4.2	*持牌人不應採納以管理儲值金額得到的投資回報為重要收入來源的經營模式。若持牌人有意以現金或銀行存款以外的低風險金融資產的形式持有某比例的儲值金額及工具按金，須事先向金管局證明有關的儲值金額及工具按金會得到充分保障，免受所有相關風險(包括投資風險、市場風險、集中風險及流動性風險等)影響，以獲得金管局的書面同意。尋求金管局事先給予同意的持牌人應至少有周全的投資政策及指引及有效的管控措施，以保障儲值金額及工具按金免受所有相關風險影響。*
附加指導	(a) 金管局在評核管控措施的成效時，會考慮的因素包括持牌人管理投資項目的專門知識及往績。
《指引》 6.4.3	*除非有有效的貨幣風險管理政策、指引及管控措施，否則除港元與美元持倉的錯配外，一般不會容許儲值金額或工具按金的計值貨幣與所持有的有關資產的計值貨幣之間的錯配。*

附加指導	(a)	若有正當理由令持牌人無法避免儲值金額及工具按金與所持的相關資產之間存在貨幣錯配，持牌人可聯絡金管局解釋有關情況。若金管局接納有需要讓有關貨幣錯配的情況存在，金管局預期持牌人會設立適當政策及程序，以監察或管理由此引起的外匯風險，以及確保有充足的儲值金額及工具按金。

7. 特定風險管理

《指引》第 7.2 條 － 科技風險管理

《指引》7.2.1	*持牌人應設立有效的科技風險管理框架，以確保：(i)資訊科技管控措施周全；(ii)電腦系統的質素及保安，包括可靠性、穩健性、穩定性及可用性；以及(iii)儲值支付工具運作的安全及效率。該框架應「適切有關目的」，即與持牌人的業務及運作性質、規模、複雜程度及類型所涉及的風險、採用的科技及整體風險管理制度相符。持牌人應在業務發展及風險管理之間適當分配其科技資源，以確保有充足資源應付後者所需。*
附加指導	在評核持牌人的科技風險管理架構的成效時，金管局會考慮以下的一般要求：

(a) 有效的科技風險管理架構通常包含妥善的資訊科技管治、持續的科技風險管理程序及實施穩健的資訊科技管控方法：

資訊科技管治

(b) 一般而言，資訊科技管治涵蓋不同範疇，包括設立架構清晰的資訊科技部門及制定資訊科技管控政策。

(c) 儘管建構可能有所不同，但典型的科技風險管理架構至少包括三個主要部門：

(i) 資訊科技部門，負責向業務單位提供日常的資訊科技服務及支援。

(ii) 科技風險管理部門，負責確保持牌人遵從穩健的科技風險管理程序(進一步詳情見下文第(e)及(f)段)，以及運用科技有效地管理其他風險，尤其是運作風險。

(iii) 資訊科技審計部門，負責確保對持牌人的資訊科技管控措施及科技風險管理程序進行充足的審計，而且所有缺失都予迅速上報、跟進及糾正。

(d) 持牌人應建立一套切合其業務模式及科技應用的資訊科

技管控政策。下文列載該套政策應具備的一些特點：

(i) 制定一套確立資訊科技管控基本原則的資訊科技管控政策。該等政策經正式批准，並由各資訊科技部門及業務單位妥善實施。

(ii) 設有清晰的程序以核實遵從資訊科技管控政策的情況，及尋求批准豁免遵守資訊科技管控政策，並訂明未能遵守有關程序的後果。

(iii) 清楚註明資訊科技部門、科技風險管理部門及資訊科技審計部門的角色及責任，以及高級管理層監察各資訊科技部門的表現的責任。

(iv) 設有清晰的程序定期檢討肩負上文第(iii)分段所述的職責的員工是否足夠及勝任(從專業知識、相關經驗及對持牌人運作的熟識程度而論)。

科技風險管理程序

(e) 持牌人應有適合其經營模式與風險狀況的有效的風險管理制度。其風險管理制度的精密程度應與持牌人業務的規模及複雜程度相符。

(f) 風險管理制度中應有穩健的程序，管理所有可能令持牌人的科技風險出現變化的改變(例如因新產品、服務、程序、合約條款引起的改變，或法律及規例等外部因素引起的改變)。有關程序應能記錄所有建議的改變，並就該等改變進行嚴格的風險識別程序。持牌人應持續嚴謹地評估、監察及管控識別到的所有風險。

實施穩健的資訊科技管控措施

(g) 持牌人應因應其經營模式與風險狀況實施周全穩健的資訊科技管控措施。金管局在評核其資訊科技管控措施是否周全時， 會考慮附件所列有關不同範疇的良好做法。

《指引》7.2.2	*鑑於無法完全消除發生資訊科技操作事件(例如服務中斷)的風險，持牌人應建立一個有充足的管理層監察的事件管理框架，以確保有效的事件回應及管理能力，能妥善應對重大事件。*

有關框架包括：(i)及時向金管局匯報任何已確認的與資訊科技相關的欺詐個案或重大保安違規事項，包括網絡攻擊、服務長時間中斷，以及系統性事件令使用者蒙受金錢損失或面對不愉快的遭遇(例如資料外洩)，以及(ii)傳訊策略以應對事件所引起任何利益關係方的關注及修補事件可能對信譽造成的損害。

附加指導

(a) 為確保事件管理架構得到充足的管理層監察，並具有充足的能力，持牌人應向負責處理任何重大事件可能引起的不同風險(例如資訊科技風險、運作風險、法律/監管風險及信譽風險)的管理層人員指派清晰的職責及賦予適當權限。該等人員應具備足夠級別。持牌人應考慮到其業務規模及複雜程度(見下文第(c)段)，以書面方式清楚界定會被視為重大事件的各類型事件。持牌人應有穩健的安排，確保就任何重大事件及時通知所有負責的管理層人員。有關管理層人員應主動互相聯絡，評估狀況及定出最恰當的行動以有效管理所有相關風險。

(b) 持牌人應致力在對其業務造成最輕微影響的情況下，盡快恢復正常的資訊科技服務。為此，持牌人應有有效的事件回應及管理程序，有關程序應至少讓持牌人能：

(i) 迅速找到事件的可能成因(例如因持牌人的保安措施或運作環境存在弱點)，以及評估事件的潛在規模及影響(例如事件會否影響其他使用者或甚至其他外部各方)；

(ii) 在切實可行的情況下盡快控制對持牌人的使用者資產、資料及信譽造成的損害，並解決有關事件，而解決的時限應與事件的嚴重程度相符。持牌人應以保障已受或可能受事件影響的使用者的權益為優先；

(iii) 迅速向高級管理層上報事件，尤其當事件可能會引致信譽受損或重大財政損失；

(iv) 迅速通知受影響使用者及(如適用)其他受影響外方(讓它們能通知其受影響的使用者)；

(v) 按需要收集及保存鑑識證據，以便利其後進行的調

查及檢控罪犯(如有需要)；

(vi) 定期匯報解決事件的進度；以及

(vii) 對事件進行事後檢討，包括識別事件成因及制定行動計劃以作出所需糾正(例如防範及偵測管控、緩減管控等)。

(c) 在典型的事件管理架構下，需要對所識別的每宗事件分配適當的嚴重程度，以能就重大事件及時作出回應。除其他事項外，須確立及記錄用作評估事件嚴重程度的準則。有關職員亦須接受充足培訓，使其能有效分辨高嚴重程度的事件。

(d) 在典型的事件管理架構下，會成立事件回應小組(成員來自相關部門)支援高級管理層人員按照既定程序管理事件並作出回應。小組的角色與責任，包括記錄、分析、補救及監察事件，有清晰界定及記錄。

《指引》7.2.3	*持牌人應有周全措施，確保為不同目的而設立的數據庫維持適當分隔，以防範未經授權或意外的存取或檢索，以及實施穩健的存取管控，以確保數據庫的保密性及完整性。就使用者(包括商戶)的任何個人資料而言，持牌人在任何時間都應遵守《私隱條例》及私隱公署不時發出的任何相關實務守則、指引或最佳行事方式。*

附加指導

(a) 持牌人應遵循私隱公署發出的相關最佳行事方式，例子包括私隱公署就互聯網網站及流動應用程式的網上追蹤功能及使用提出的建議。

(b) 一般而言，為保障數據庫的保密性及完整性，除其他措施外，持牌人應實施以下管控措施：

(i) 由一套設有存取管控規則的周全認證機制，限制對資料及應用系統的存取。採用以職責為本的管控架構，只按需要授予存取權。

(ii) 成立保安管理部門及制定正式程序，以管理系統資源及應用系統的存取權分配，並監察系統資源的運

用，以偵測任何異常或未經授權活動。

(iii) 對保安管理部門或其他輔助管控措施(如同級評審)的職責實施適當劃分，以減低保安管理部門進行未經授權活動的風險。

(c) 小心謹慎地管控特許及緊急識別碼的運用及存取。在一個典型的情況下，必要的管控程序包括：

(i) 更改預設密碼；

(ii) 限制特許使用者的數目；

(iii) 對特許使用者進行遠端存取實施嚴格管控；

(iv) 只向具有特許及緊急識別碼的人士授予屬絕對必要的權限；

(v) 由適當的高級人員給予正式批准後才可運用；

(vi) 記錄、保存及維持具有特許及緊急識別碼的人士所進行的活動(例如對活動記錄進行同級核審)；

(vii) 禁止分享特許帳戶；

(viii) 妥善保管特許及緊急識別碼及密碼(例如保存於密封信封，放在數據中心，並鎖好)；以及

(ix) 在使用特許及緊急識別碼的密碼的人士交還密碼後即時更改密碼。

《指引》 第 7.3 條 － 支付保安管理

《指引》7.3.2	*持牌人應就資料所有權、分類、儲存、傳送、處理及保留有周全的政策及程序，以確保透過登記使用儲值支付工具服務及執行支付交易而從使用者收集所得的資料的保密性及完整性。*
附加指導	金管局在評核支付保安管理政策及程序是否周全時，會從資訊科技及非資訊科技角度考慮以下各項：

(a) 資料所有權

就持牌人所收集、處理、創設及維持的資料而言，持牌人應指派專責人士作為資料所有人。一般而言，該資料所有人負責系統所處理及儲存的資料的分類、使用授權及保障。

(b) 資料分類

資料應按照敏感程度分類，以反映所需的保障程度。為協助分類過程，持牌人應就每種類別制定指引及定義，並按照分類計劃定出適當的保障資料程序。

(c) 已儲存的資料

儲存於終端用戶裝置及儲值支付工具持牌人後端系統中的敏感資料(如支付數據、個人身分識別資料及認證資料)應予以適當保障，以防範盜竊及未經授權存取或修訂。有關資料應以有力及獲廣泛認可的加密技術予以加密，並儲存於安全的儲存環境內。此外，正式接納程序應包括妥善的測試個案，以確保涵蓋所有有關保障該等資料的管控措施(例如防範電子扒手的管控措施)。

(d) 傳送中的資料

持牌人應確保在傳送敏感資料(例如由使用者的裝置至持牌人的伺服器)時，以有力及獲廣泛認可的加密技術，並採用及維持有力及安全的端對端加密，以保障資料的保密性及完整性。

如適用，交換資料的通訊渠道只應按需要開放。例如若切實可行，透過非接觸式渠道進行的通訊只可在使用者啟動後及在限定的時限內作出。

(e) 處理中的資料

若持牌人提供收單服務，應要求其商戶設有必要措施以保障與支付相關的敏感資料，以及避免向未能確保有關保障的商戶提供服務。持牌人亦應實施充足措施，以維持

及核實其系統所處理的資料的完整性。

(f) 資料的保留及處置

持牌人應根據適用法例、監管規定及業務要求，實施資料保留及處置政策，限制資料存量及保留時間。持牌人應有程序安全地刪除不再需要的資料。

(g) 資料最少化

持牌人在設計、發展及維持支付服務時，應確保資料最少化是核心功能的重要原則之一：敏感資料的收集、傳送、處理、儲存及/或存檔及視覺化應維持在最低水平。不必要的資料不應在不需要有關資料的系統及處理程序中呈列。例如持牌人可能在其後端系統中持有的使用者帳戶資料(例如持卡人姓名)不應儲存於無需該等資料以完成交易的使用者所控制的前端裝置或應用程式內，亦不可經由該等裝置或應用程式存取。此外，儲存於使用者裝置的其他應用程式應不能存取持牌人的支付應用程式所使用的資料(即「應用程式沙盒」或「應用程式容器」)。

《指引》7.3.3	*持牌人應實施周全的保安措施，以保障提供予使用者運用其儲值支付工具的每個支付渠道(包括卡及使用者裝置)，免受所有重大弱點及攻擊影響。*
附加指導	金管局在評核支付渠道的保安措施是否周全時，會考慮以下各項：

(a) 支付卡

提供支付卡服務的持牌人應實施周全的保障措施，以保障敏感的支付卡資料，例如利用晶片卡儲存該等資料，並就銷售點及自動櫃員機的卡交易實施強力的認證方法。根據風險為本方法，就限額較高及功能較多的卡(如客戶身分已經核實的卡)而言：

(i) 實體卡應內置晶片，除非該卡附有與未經核實的卡(或禮品卡)相同的特點；

(ii) 如實體卡可用作進行本地自動櫃員機交易，應實施晶片認證；以及

(iii) 若實體卡可用於在境外自動櫃員機提取現金，應實施有效的風險管理措施(如較低的交易限額、通知安排、騙案監察，並具備可讓客戶啟動/解除相關功能，以及能下調提款限額的彈性)。

(b) 使用者裝置

持牌人應假設使用者裝置會面對保安風險，並在設計、發展及維持支付服務時採取適當措施。持牌人應有保安措施，以防範不同情況，包括未經授權裝置存取、惡意程式或病毒攻擊、流動裝置受感染或沒有保安措施，以及未經授權流動應用程式。

(c) 以流動裝置接納支付

若商戶使用流動裝置接納持牌人的支付辦法，應實施額外保安措施以保障流動支付接納辦法，包括偵測異常活動，並在報告中記錄，以及提供商戶身分資料以供使用者核實其身分。

(d) 非接觸式支付[2]

為防範潛在惡意攻擊，以及應對洩漏數據、使用者遺失或被盜取裝置/卡的風險，持牌人應就非接觸式支付實施周全及有效的保安管控措施，包括以下各項：

(aa) 進行非接觸式支付所需的敏感資料應以安全方式儲存及存取；

(ab) 非必要數據應以不會輕易被未經授權人士獲取的方式儲存；

(ac) 如支付資料可能受到轉發/中繼攻擊，應實施額外管控措施(如額外認證條件、較短的動態支付資料有

[2] 非接觸式支付指利用非接觸式或無線技術(如二維碼或近場通訊技術)在客戶的裝置(如實體卡、流動裝置)及收款人(如商戶)之間傳遞支付資料(如支付卡資料)。

效期或較低的支付限額)；以及

(ad) 就可用作在銷售點進行非接觸式支付的靜態支付資料而言，應禁止使用該等支付資料在非銷售點進行交易，除非該等支付資料在進行非接觸式交易時不會面對被未經授權人士獲取的風險。

持牌人應實施周全及有效的保安管控措施，以防範及偵測未確認/不完整交易(如因干擾或其他運作原因)，以及協助及時向客戶退款。

《指引》7.3.4	*持牌人應實施周全的支付保安措施，以確保支付交易的真確性及可追蹤性，以及偵測欺詐交易。*
附加指導	金管局在評核《指引》第7.3.4條所載的保安措施是否周全時，會考慮以下各項：

(a) 使用者認證

(i) 在考慮使用單一認證條件或多重認證條件時，持牌人應顧及在通過認證後可以進行的運作涉及的風險，包括遵守以下規定：

(aa) 在採用及其後定期考慮有關認證條件或多重認證條件的成熟度及成效；

(ab) 就登記、更改及取消認證條件實施有效管控措施，以確保有關變更是由真正的使用者妥為作出；

(ac) 若使用電子證書為認證條件之一，確保有關電子證書及相關鑰匙(如適用)為不可複製，並以安全方式儲存；以及

(ad) 就電子錢包而言，若認證條件是由安裝了電子錢包的相同流動裝置推演出來、可於相同裝置查閱或存取(如使用者可使用相同的流動裝置接達電子錢包及收取以短訊形式發出的一次性密碼或生成一次性密碼)，認證的成效

便會減弱，持牌人應考慮於不同情境下的風險狀況實施相稱而有效管控措施。例子包括要求與有關流動裝置無關的認證條件及/或實施其他有效管控措施(如加強詐騙監察、下調儲值/交易限額及限制功能/特點)。

(ii) 持牌人應選用可靠及有效的認證方法，以核實其使用者的身分及授權。若合併使用以下三個因素中的任何兩個或以上，使用者認證會更具效力(即雙重認證)：

(aa) 使用者已知的資料(例如使用者的識別碼及密碼)；

(ab) 使用者擁有的工具(例如由保安顯示器或持牌人的保案系統發出只可使用一次的密碼)；以及

(ac) 使用者本身的特徵(例如視網膜、指紋或聲音辨識)。

(iii) 若密碼(包括個人識別號碼(PIN))被用作其中一項認證因素，持牌人應就密碼的強度有健全的管控措施(例如最起碼的密碼長度)。

(iv) 若以一次性密碼作為認證條件，持牌人應遵守以下規定(如適用)：

(aa) 實施穩健的主要管理方法以保障生成一次性密碼的暗碼(如種子值)；

(ab) 定期評估一次性密碼是否周全及有效；

(ac) 加入充足資料，讓使用者能識別一次性密碼的目的及相關的交易；

(ad) 在容許使用者更改收取一次性密碼的手機號碼或裝置前，進行適當及有效認證；以及

(ae) 若利用以短訊形式發出的一次性密碼，作出必要安排，確保即使啟動了轉傳短訊功能，以

短訊形式發出的一次性密碼亦只會傳送至已登記手機號碼。

(b) 登入嘗試及登入狀態管理

(i) 有效的管控措施包括限制嘗試登入或認證的次數(例如錯誤輸入密碼的次數)、實施超時管制及就認證的有效期設定時限。若以只可使用一次的密碼作認證，持牌人應限制該密碼的有效期在必要的最短時間內。

(ii) 若就嘗試登入或認證的次數實施了限制，而失敗嘗試的次數已達到有關限額，應暫停或永久停用支付服務。沒有活動的支付服務登入狀態亦應在預設最長時間後自動終止。

(c) 記錄活動

(i) 持牌人應有程序確保記錄所有交易，並有適當的審計記錄。其服務應併入保安機制以詳盡記錄交易資料(包括交易編號、時間戳、參數設置的修改及交易資料的存取)。

(ii) 持牌人應有穩妥的記錄檔案以供檢索以往的資料，包括交易的增加、修改或刪除的整全審計記錄。只有獲授權人士方可使用該等工具(包括特許責任)，並應適當記錄。

(iii) 若可透過不同渠道進行支付，有關檔案應可清楚識別有關支付渠道。持牌人亦應識別及記錄支付交易的來源(例如銷售點、互聯網)及收款人。

(iv) 持牌人應為使用者提供渠道，以查核其以往的交易。若使用有關渠道須收費，金額應合理，並應通知使用者。

(d) 欺詐偵測系統

(i) 持牌人應設立交易監察機制，以防範、偵測及阻止欺詐支付交易。可疑或高風險交易應經過特定的篩查、

篩選及評核程序。

(ii) 若儲值支付工具允許使用者以綁定信用卡/扣帳卡/預付卡作為其儲值支付工具帳戶的資金來源，持牌人應實施適當安排，由相關發卡機構向持卡人進行認證(例如以短訊形式發出一次性密碼或其他有效措施)，確認該持卡人已同意綁定有關信用卡/扣帳卡/預付卡。儲值支付工具至少應在使用者進行綁卡或第一次使用該卡進行交易時啟動上述認證安排。若相關發卡機構並不支援持牌人所要求的認證安排，或未能與有關持卡人進行所須認證，持牌人應拒絕接受綁定有關的信用卡/扣帳卡/預付卡。

(iii) 若儲值支付工具允許使用者設立由銀行帳戶直接扣帳至其儲值支付工具帳戶的指示，持牌人應實施適當措施，以確認該扣帳指示已獲得有關銀行帳戶持有人的授權。就此，持牌人應參考金管局於 2018 年 10 月 26 日頒布的相關措施及其他適用指引。

(iv) 若持牌人按照其風險政策，決定阻止某項被識別為具有潛在欺詐成分的支付交易，持牌人應盡可能維持最短的阻止時間，直至有關的保安事宜得到解決。持牌人的監察機制應能迅速通知其監察人員有可疑的網上轉帳及異常活動。在該等情況下，持牌人應盡快向使用者查核該等交易或活動。

(v) 持牌人應實施有效措施，以防範駭客透過自動化工具在客戶登入帳戶過程中進行自動化蠻力攻擊及憑證填充攻擊。

(e) 維持帳戶

(i) 持牌人應就高風險的帳戶維持功能(如更改密碼、重設密碼、要求或更改已登記裝置及更改收取以短訊形式發出的一次性密碼的手機號碼、更改經核實帳戶擁有人、提高交易限額等)，實施適當保安管控措施及認證。其中一項良好做法是持牌人應提醒在一段較長期間內維持密碼不變的使用者定期更改密

碼。

(ii) 持牌人應就在一段較長期間內沒有進行任何交易的帳戶(不動帳戶)實施額外管控措施。例如持牌人可停止不動帳戶的支付功能，直至確信該帳戶是繼續由真正的使用者使用。

(f) 帳戶整合服務

(i) 為妥善管理透過與其他機構合夥提供的帳戶整合服務[3]可能產生的相關風險(如法律、信譽及業務操作風險)，持牌人應在推出有關服務前實施有效管控措施，包括但不限於以下各項：

(aa) 進行獨立法律盡職審查；

(ab) 實施適當管控措施以保障客戶，如處理客戶投訴及客戶可能蒙受的任何財政損失的責任分配等；

(ac) 確保遵守適用的本地或境外法律及監管規定，包括個人資料私隱規定(如適用)；

(ad) 評估及消除因與夥伴機構的任何聯繫而導致持牌人系統及網絡入侵的風險；以及

(ae) 向客戶妥為披露帳戶整合服務的風險及限制。

《指引》7.3.5	*持牌人應核實儲值支付工具使用者的身分，才讓其管理其儲值支付工具帳戶及進行高風險交易，並應在有關活動後及時向使用者發出通知。*
附加指導	金管局在評核持牌人遵守《指引》第7.3.5條的情況時，會考慮以下各項：

[3] 若持牌人提供帳戶整合服務，一般是容許使用者透過持牌人營運的電子錢包或平台接達於其他機構(可以是境外機構)開設的帳戶，而無需使用者另行登入該等機構的平台。

(a) 使用者帳戶的管理

(i) 若持牌人容許使用者透過網上渠道開設帳戶，應採用可靠方法核實使用者的身分。

(ii) 持牌人應在使用者要求更改帳戶資料或聯絡資料(有關資料可供使用者用作收取重要資訊或監察其帳戶的活動)時，充分查核使用者的身分。此外，持牌人應採取措施防範及偵測與有關更改可能涉及的欺詐情況。

(b) 對高風險交易的管控

(i) 持牌人在決定哪些交易類型屬高風險交易時，應顧及交易的風險狀況及評估，以及認證方法的成效等相關因素。持牌人在每次執行高風險交易前，在情況許可下，都應進行與該等風險相稱的有效的管控措施，如雙重認證或其他減低風險的措施，以重新核實使用者身分。高風險交易至少應包括：

(aa) 超越預設交易限額的交易；

(ab) 更改可讓使用者監察其帳戶活動的個人聯絡資料；

(ac) 超越合計滾動限額(即在一段時間內的交易總額)的交易，除非不可能就有關的儲值支付工具落實執行有關管控；

(ad) 為收取一次性密碼或通知等目的而綁定社交媒體帳戶；

(ae) 啟動可以無需提供個人身份識別號碼(PIN)亦可進行支付的功能(僅可用於商戶支付)[4]；以及

(af) 在電子錢包展示使用者的所有聯絡資料或二

[4] 就此情況而言，持牌人亦應讓客戶清楚知悉其已啟動此功能。此規定亦適用於在開戶時已預設啟動此功能的情況。為施行此規定，無需提供個人身份識別號碼亦可進行支付的功能一般不應用作進行個人對個人交易。

維碼。

(ii) 持牌人應界定每宗交易的限額，同時除非不可能就有關的儲值支付工具落實執行，否則亦應在考慮其欺詐監察能力、每個儲值支付工具的最高儲值額(如適用)、每日增值上限(如適用)及所實施的其他防範欺詐的保障機制後界定滾動限額。持牌人應清楚通知使用者有關限額。

(c) 向使用者發出通知

(i) 為能及時偵測可能因欺詐活動而引起的未經授權交易，一旦使用者進行高風險交易或超使用者在其帳戶設定的限額(如適用)的交易時，持牌人應盡可能立即通知使用者。交易提示應包括交易的來源及金額等資料，以協助使用者識別真正的交易。

(ii) 持牌人在決定哪些交易類型應在完成後透過有效渠道向使用者發出通知時，應顧及交易的風險狀況及評估。作為一般參考基準，以下交易類型應發出通知：

(aa) 並非在銷售點進行的交易(如無卡交易)；

(ab) 高風險二維碼支付；

(ac) 高風險境外銷售點交易；

(ad) 高風險自動櫃員機提款交易；

(ae) 可疑帳戶登入或未經雙重認證的帳戶登入；

(af) 更改支付限額；

(ag) 啟動可以無需提供個人身份識別號碼亦可進行支付的功能；

(ah) 更改聯絡資料；

(ai) 更改認證方法；

(aj) 在沒有提供個人身份識別號碼的情況下進行

支付(僅限於非實體形式的支付)；以及

(ak) 未經雙重認證便轉帳資金至第三方(僅限於非實體形式的轉帳)。

(iii) 在決定選用哪種通知渠道(如短訊、電郵或 in-app 通知)時，持牌人應考慮交易的風險及有關渠道的成效。若選用短訊通知，持牌人應與流動網絡營運商實施相關管控措施，以確保有關的短訊通知能傳送至已預先登記的手機號碼及轉傳香港手機號碼(如使用者已就其手機號碼啟動轉傳短訊服務)。

(iv) 若使用者要求持牌人不作出有關通知，持牌人應確保設有妥善適當的程序及步驟，包括：

(aa) 向使用者解釋如不向使用者發出有關通知的潛在風險及任何對其他服務造成的影響，並要求使用者確認其了解相關風險及影響；

(ab) 妥為認證使用者身分，確保有關要求是由真正的使用者提出(如適用)；

(ac) 若有關使用者要求接收有關通知，應接受有關要求；以及

(ad) 就上述程序備存妥善記錄。

《指引》7.3.6	*持牌人應透過有效的通訊渠道，就安全使用儲值支付工具向使用者提供意見及協助。*
附加指導	金管局在評核持牌人是否遵守《指引》第7.3.6條時會考慮以下各項：

(a) 向使用者提供的保安提示

(i) 持牌人應提醒使用者，他們有責任採取合理的保安措施以保護其用於支付的裝置，以及妥善保管及保密其支付服務的密碼。此外，持牌人應透過有效的方法及多個渠道，向使用者提供易於明白、顯眼及定期予以檢討的保安措施提示。

(ii) 此外，持牌人應管理有關欺詐電郵、網站及流動應用程式誘使使用者透露敏感使用者資料（如登入識別碼、密碼及只可使用一次的密碼）的風險。尤其持牌人應定期搜尋互聯網及應用程式商店(App stores)，查看是否有虛假或可疑網站或應用程式。若持牌人發現任何會令公眾誤會是來自持牌人的虛假或可疑電郵、網站或應用程式，或可由非正式渠道下載其應用程式，持牌人應及時決定是否需要知會其使用者及公眾，以及向警方及金管局舉報有關事宜。

(b) 與使用者聯繫

(i) 持牌人應提供至少一個安全渠道，就正確及安全使用支付服務與使用者保持聯繫。持牌人應知會使用者此一渠道，並說明任何透過其他方式代表持牌人發出的訊息都不可靠。持牌人應透過該安全渠道通知使用者有關支付服務保安措施的最新資訊。任何有關新出現的重大風險的提示亦應透過這個安全渠道提供予使用者。

(ii) 持牌人應就所有問題、投訴、支援要求及有關支付及相關服務的異常情況或事件的通知為使用者提供協助，並應適當知會使用者有關如何在可能有第三方參與的情況下取得有關協助。

《指引》7.3.7	*持牌人應監察網絡威脅的趨勢、實施周全的保障措施及定期進行保安測試，以防範目前及日後可能出現涉及其儲值支付工具的網絡保安風險。*
附加指導	金管局在評核持牌人是否遵守《指引》第7.3.7條時，會考慮以下各項：

(a) 網絡保安風險管理程序

若持牌人非常倚賴互聯網及流動技術提供服務，則應透過持牌人的科技風險管理程序妥善管理網絡保安風險。持牌人亦應投放足夠資源以確保有能力識別風險、保障其關鍵服務免受攻擊、控制網絡保安事件的影響並恢復

服務。

(b) 網絡威脅資訊

持牌人應緊貼網絡威脅的趨勢，並可考慮訂購與其業務相關的優質網絡威脅資訊服務，以加強其及時精確地應對新類型的威脅的能力。持牌人亦可尋求機會與其他機構共享及收集網絡威脅資訊，以使儲值支付工具業界能更有效應對及管理網絡保安風險.

(c) 滲透測試

持牌人應定期評估進行滲透測試的需要。測試內容及範圍應以網絡保安風險狀況為依據，不僅涵蓋網絡(外部及內部)及應用系統，亦應包括社交工程威脅及新出現的網絡威脅。持牌人應根據影響及風險承擔分析的結果，及時採取適當行動，以減輕在滲透測試中所發現的問題、威脅及弱點。

(d) 互聯網連接裝置

隨着互聯網演變，越來越多裝置或設備內置可連接互聯網的功能。這些裝置的網絡連接功能經常處於「啟動」狀態，可能會構成更多端點讓滲透者可進入持牌人的關鍵資訊科技基礎設施。持牌人應留意相關風險，並採取相應的適當措施。

《指引》 7.3.8	*持牌人應提供與其儲值支付工具運作模式相符的具效率及可靠的儲值支付工具支付服務。*
附加指導	(a) 一般而言，效率及可靠程度應按可量度的效能指標評核，例如回應時間、交易處理量、系統容量、系統可用性及穩定性。持牌人應參照有關效率及可靠性的預設指標測試及監察其儲值支付工具。就高效能要求的服務商戶(例如公共運輸服務提供者)的儲值支付工具而言，持牌人應與有關商戶議定預期效能指標，並投入充足資源以確保符合有關指標。

《指引》第 7.4 條 － 持續業務運作管理

《指引》 7.4.1	*持牌人應有周全的持續業務運作管理計劃，以確保一旦因不同情況引致重大干擾時可繼續或及時恢復其關鍵運作，或在極端情況下有序縮減其關鍵運作的規模。*

附加指導

(a) 一般而言，周全的持續業務運作管理計劃包括業務影響分析、恢復策略、業務持續運作計劃及業務及資訊科技運作復原的備用場地。下文載有相關說明。

業務影響分析

(b) 業務影響分析通常包括兩個階段。第一階段是(i)識別可能會在一段時間內(可長可短)令持牌人的服務中斷的潛在情況；以及(ii)識別在服務中斷一段較長時間的情況下，必須維持的最低程度的關鍵服務。

(c) 第二階段的業務影響分析是時限評估，目的是制定切合實際、可量度及可達到的主要恢復運作時間目標：(1)恢復最低程度的關鍵服務前可容忍的最長停止運作時間；(2)關鍵資訊科技資源的恢復運作時間目標；以及(3)回復資料的恢復點目標。

(d) 持牌人應考慮從科技風險事件及經營環境的變化(例如科技應用的變化、新產品/服務的提供、業務規模顯著擴大等)所得到的啟示，定期檢討業務影響分析。

恢復策略

(e) 持牌人應有一套恢復策略，而有關策略應有清晰文件記錄、經全面測試及定期演習，以確保能達到恢復目標。

(f) 其中一項關鍵的服務恢復元素是穩妥完善的記錄管理。持牌人應有有效措施，以確保所有業務記錄，尤其是使用者記錄，一旦遺失、受損或遭破壞，可及時修復。重要的是，持牌人須容許使用者及時存取其本身的記錄。

(g) 持牌人在決定最低服務水平及恢復目標時，應考慮多項相關因素，包括但不限於關鍵服務/系統的相互倚賴程度、使用者及其他利益關係方對其服務的速度、穩健性及可靠性

的要求，以及法律及信譽風險的影響。

業務持續運作計劃

(h) 一般預期業務持續運作計劃包括：(i)啟動觸發服務恢復策略的詳細程；(ii)遇到嚴峻或長時間的服務中斷情況時的上報程序及危機管理程序(例如設立指揮中心、及時向金管局匯報)；(iii)積極主動的通訊策略(例如通知客戶、回應傳媒) ；(iv)參與業務持續運作計劃的主要人員的最新聯絡資料(應提供予金管局)，以及(v)就關鍵系統的恢復指派主要及輔助負責人員。

業務及資訊科技運作復原的備用場地

(i) 場地挑選

(i) 持牌人應檢視主要業務部門集中於相同或鄰近地點的程序，以及備用場地與主要場地的距離。備用場地應與主要場地保持一定距離，以免受相同的災害影響。

(ii) 持牌人的備用場地應易於進入，配備適當設施於業務持續運作計劃指明的時間要求內可供佔用，以及實施適當的進入場地管控。持牌人亦應特別留意將運作遷至備用場地的交通運輸安排。

(j) 資訊科技運作復原的備用場地

(i) 資訊科技復原的備用場地應有充足的技術設備（包括通訊設備），以應付復原要求。該設備應為適當型號及有適當容量。若持牌人的主要外方的主要場地鄰近持牌人的主要場地，應考慮在其備用場地與該等主要外方的備用場地之間建立通訊聯繫。

(k) 由供應商或其他機構提供的備用場地

(i) 持牌人應避免過度倚賴外部供應商提供業務持續運作支援。持牌人應能確信該等供應商有能力在有需要時提供服務，並應清楚註明供應商的合約責任，包括提供支援的時間、類型及容量等。

(ii) 若持牌人倚賴外部提供者提供的共用電腦服務(例如雲端運算)以支援其災難復原，應管理該等服務所涉及的風險。有關資訊科技外判指引，見「外判管理」部分。.

《指引》7.4.2	*持牌人的董事局及高級管理層對業務持續運作管理及業務持續運作計劃的效用負有最終責任。持牌人的董事局及高級管理層應確保業務持續運作管理計劃妥善落實，各級員工都認真對待有關計劃，並投放充足資源實施計劃。*
附加指導	金管局在評估核牌人的董事局及高級管理層有否履行《指引》第7.4.2條所述的職責時，會考慮以下各項：

董事局及高級管理層的監察

(a) 確立責任

(i) 持牌人的高級管理層應清楚確立哪個部門負責管理整個業務持續運作管理程序，以及確保該部門有充足的資源及專門知識。

(b) 監察、匯報及批准

(i) 業務持續運作管理部門應定期向董事局及高級管理層提交有關業務持續運作計劃測試的報告，以及向高級管理層匯報有關業務持續運作計劃的任何重大改動。

(ii) 董事局及高級管理層應確保審計周全地涵蓋其業務持續運作計劃，以確定計劃是否切合實際、繼續適用，以及符合持牌人訂立的政策及標準。

(iii) 鑑於業務持續運作管理的重要性，持牌人的行政總裁應就所採納的恢復策略是否仍然有效，以及所記錄的業務持續運作計劃是否經過妥善測試及維持，編製及簽署正式的周年聲明，以提交董事局。

業務持續運作計劃的實施

(c) 測試及演習

(i) 持牌人應至少每年一次測試其業務持續運作計劃。高級管理層、主要及候補相關人員應參與周年測試，以熟習其在恢復運作中的責任。

(ii) 在計劃周年測試時，持牌人應檢視所有業務持續運作計劃的相關風險及假設，確保其仍然適合。持牌人亦應編製正式測試文件(包括測試計劃、設想的情況、程序及結果)，以及事後檢討報告，供高級管理層正式簽署作實。若測試結果顯示業務持續運作計劃存在弱點或漏洞，應更新有關計劃及恢復策略以糾正有關情況。

(d) 定期保養

(i) 持牌人應有正式的變動管理程序，以確保其業務持續運作計劃因應任何相關變化作出修訂。若計劃被啟動，持牌人應在恢復正常運作後，立即作出檢討，以識別可作出改進的地方。若需要供應商提供重要恢復運作服務，應定期檢討服務水平協議。

(ii) 業務及支援部門應在業務持續運作管理部門的協助下每年檢討其業務影響分析及恢復運作策略，以確認業務持續運作計劃要求的有效性。

(iii) 在接獲有關主要人員、對手、使用者及服務提供者的聯絡資料的更改通知後，應盡快予以更新。

(iv) 業務持續運作計劃文件的副本應儲存於主要場地以外的地點。在緊急情況下應採取的主要措施概要應提供予高級管理層及保存於多個地點。

8. 經營手法及操守

《指引》第 8.2 條 － 操守標準及經營手法

《指引》 8.2.3	*持牌人應確保其採納及(如有需要)制定能反映其操守標準的良好經營手法。*
附加指導	(a) 一般而言，持牌人至少應採納以下經營手法： (i) 持牌人應進行盡職審查，以確保其發出的所有宣傳資料都正確，沒有誤導成分； (ii) 持牌人可運用其網站及流動應用程式提供與電子商貿入門網站及其他網上商戶的連結。若提供該等連結，持牌人應管理信譽風險，對有關的電子商貿入門網站及商戶進行盡職審查，以確定其為真正的公司，從事正當合法的業務；以及 (iii) 持牌人的網站或應用程式可提供超連結連至提供金融產品及服務的顧問及/或銷售服務的其他網站。惟持牌人應尋求外聘法律意見，以確保有關安排符合所有有關法律及監管規定。持牌人應列明有關產品及服務由第三方提供，並在其網站或應用程式加入免責聲明，說明該等超連結與其儲值支付工具業務無關，同時有關產品及服務並未獲持牌人或金管局或任何其他主管當局認可。
《指引》 8.2.4	*持牌人不得根據儲值金額的多寡提供利息或類似利息的獎勵計劃。*
附加指導	(a) 為免引起疑問，持牌人可以提供並非以儲值金額的多寡為依據的獎勵計劃，例如以交易為基礎的計劃。然而，持牌人應確保並能證明在商業上有關計劃可行及可持續。持牌人應進行嚴格的分析，確保其計劃的預算影響受到嚴格控制。

《指引》第 8.3 條 － 計劃及運作規則

《指引》 8.3.1	*儲值支付工具的運作規則對所有有關各方都應公平。持牌人應嚴格按照有關的運作規則運作其儲值支付工具計劃。*

附加指導

(a) 儲值支付工具計劃的運作規則應涵蓋儲值支付工具的整體業務運作，包括但不限於使用者帳戶的開立及維護；商戶收單服務及與業務合作夥伴的協議關係；交易前後及付款授權程序。

(b) 若持牌人擬引入業務合作夥伴(例如聘用收單機構拓展受理商戶)，應確保與該業務合作夥伴的安排不會影響持牌人履行《支付條例》下有關儲值支付工具運作安全及有效率的規管義務，尤其：

(i) 持牌人與該業務合作夥伴建立業務關係前，應進行盡職審查仔細評估當中涉及的風險，並設立周全的管控機制以減低所識別之風險；

(ii) 持牌人應透過訂立清晰的服務水平協議，清楚列明雙方就有關業務安排的相關義務及責任，以有效制訂和執行其與業務合作夥伴的協議關係。同時，協議關係亦設有所需保障措施以確保儲值支付計劃的運作安全及效率。如涉及商戶收單服務，持牌人亦應確保該收單機構與商戶的協議關係符合上述要求；

(iii) 持牌人應實施適當管控及監察其與業務合作夥伴的業務安排 (例如屬收單機構，應確保該收單機構有妥善制度處理與商戶的款項交收)，並減低任何潛在的洗錢及恐怖分子資金籌集風險；以及

(iv) 持牌人應確保其與業務合作夥伴的安排符合《私隱條例》及有關保障資料的相關監管指引，以保障其使用者的利益。

《指引》8.3.4

持牌人應清楚列明及解釋其計劃、工具、服務及產品的主要特點、風險、條款及條件，以及適用收費、費用及佣金，並以有效的方法傳達及提供予有關使用者(包括商戶)。持牌人應制定額外披露事項，包括適當的警告，以提供與其計劃、工具、服務及產品的性質、複雜程度及風險相符的資料。尤其就該計劃與使用者訂立的有關合約應清楚及顯眼地列明應支付的費用及收費金額，以及須支付有關費用及收費的情況。

附加指導	(a) 持牌人應按照符合《私隱條例》的規定及私隱公署不時發出的任何相關實務守則、指引及最佳做法的方式，清楚列明其個人資料政策及做法。 (b) 如有需要，持牌人應提供方法讓使用者在簽約使用有關服務/產品前，確認已閱讀有關使用該等服務/產品的主要資料及披露事項。例如在載有主要披露事項的網頁提供確認選項，讓使用者藉選取有關選項聲明已閱讀其中所載的披露事項。
《指引》8.3.5	*持牌人應對其儲值支付工具計劃的穩健性負全責，因此應全數承擔 在使用者並無錯失的情況下使用者帳戶所儲價值的損失。*
附加指導	(a) 持牌人在所有情況下都應遵守《指引》第8.3.5條。除非持牌人能證明使用者以欺詐方式行事、嚴重疏忽(例如未能妥善保障讓其儲值支付工具服務/產品的卡、裝置或密碼)在發現或相信其帳戶(例如使用儲值支付工具服務/產品的卡、裝置或密碼)資料外洩、已遺失或被盜取或發現或相信經其帳戶進行了未經授權交易後未能在切實可行情況下盡快通知持牌人，否則使用者不應對經其帳戶進行的未經授權交易而蒙受的任何直接損失負責。

《指引》第 8.4 條 － 投訴處理

《指引》8.4.2	*持牌人的投訴管理制度應全面、具透明度、可供儲值支付工具使用者使用及易於啟動、公平公正、貫徹其提供補救的方法、具彈性及效率，以及能維持適當的保密性、備存充足紀錄、解決投訴、識別及糾正投訴所反映的問題，並向金管局作出適當回應。*
附加指導	在評核持牌人遵守《指引》第 8.4.2 條的情況時，金管局一般會考慮以下各項，並考慮持牌人的業務規模及複雜程度： (a) 有全面及具透明度的投訴處理政策，讓投訴可以迅速、客觀、公平、一致及保密的方式得到處理；以及有適當的管理措施，監察遵守及妥善實施有關政策及程序的情況； (b) 有關提出投訴的方法及地點應清晰、明確，投訴人可易於到訪及明白。有充足渠道及方法讓投訴人提出投訴，並應

以周全及及時的方式向投訴人適當地確應投訴，並告知其跟進行動、回應及結果；

(c) 有有效的政策及程序以確保投訴人的私隱。其中包括清晰的程序以保障投訴人的身分，同時確保與投訴人相關的資料僅限於有需要知道的負責員工才會知悉；

(d) 投放充足資源(包括具備相關技能、培訓、授權及獨立性的員工)，以確保投訴得到有效及迅速的處理及跟進，以及有有效機制讓持牌人的高級管理層監察投訴處理的進度及過程；

(e) 若投訴得到確立，要在合理期限內向投訴人提供滿意的補救及糾正方案，並建立有效的制度以能在考慮到投訴的相關情況及性質後決定有關的補救及糾正方案；以及

(f) 有清晰的投訴處理問責制度，並以投訴為推行進一步改進組織架構及運作的機會。有關投訴及處理程序的事實、通訊及有關詳情的全面而準確的記錄應保密處理，並保存一段適當的時間。當金管局提出相關要求時，持牌人應能提供有關記錄予金管局。

附件

資訊科技管控措施的良好做法

資訊系統的開發及收購

(a) 項目管理

(i) 就主要科技相關的項目(如內部軟件開發及收購資訊系統)建立一般管理框架。該框架註明所採用及應用於有關項目的項目管理方法。

(b) 項目發展周期

(i) 採納並實施全面的項目發展周期方法，規管開發、實施及維修保障主要電腦系統的程序。

(ii) 有關的項目發展周期方法清楚界定項目小組的角色及責任，以及每個階段可達到的目標。

(iii) 若持牌人從供應商收購軟件套裝組合，建立正式的軟件套裝組合收購程序，以管理與收購有關的風險，例如違反軟件牌照協議或專利侵權等。確保軟件供應商為軟件套裝組合提供持續維修保養及足夠支援，並在正式合約內列明有關服務。

(iv) 由獨立人士(如有需要，在法律及合規部門協助下)對主要科技相關的項目進行質素保證檢討。

(c) 保安要求

(i) 在系統開發或收購初期，清楚訂明保安要求為業務要求的一部分。在開發期間建立有關保安措施，並在測試後實施。

(d) 編碼方法

(i) 參考業內有關安全開發的公認方法，制定軟件開發的指引及標準。

(ii) 可以風險為本的方式實施源碼檢討(例如同業檢討及自動化分析檢討)，作為軟件質素保證程序的一部分。在系統啟用前識別及解決系統弱點及編碼方法不合規的情況。

(e) 系統測試、驗收及運用

(i) 建立正式的測試及驗收程序，確保只有經過妥善測試及批准的系統才會

推出至作業環境使用。測試範圍應涵蓋商業邏輯、保安管控措施及在不同壓力負載情況及恢復條件下的系統表現。

(ii) 維持獨立的開發、測試及作業環境，並在測試環境中妥善進行系統測試及用戶驗收測試。

(iii)作業數據除非已刪除其中的敏感數據，並已事先取得資料所有人的批准，否則不得用於開發或驗收測試。

(iv)在系統啟用前由獨立人士妥善進行滲透測試。

(f) 職責劃分

(i) 應妥善分隔各資訊科技小組的職責。負責開發的人員不能進入接達作業資源庫及對作業環境引入程式編製代碼。供應商進入用戶驗收測試環境(如有需要)受到緊密監察。

(g) 終端用戶電腦應用

(i) 維持由終端用戶開發的軟件清單，並按需要建立有關終端用戶電腦應用的管控方法及責任，例如所有權、開發標準、數據保安、文件紀錄、數據/檔案儲存及備份、系統恢復、審計責任及培訓等。

<u>資訊科技服務支援</u>

(h) 問題管理

(i) 建立問題管理程序以及時識別所有資訊科技問題，並予以分類、定出優先次序及加以解決。清楚定明參與問題管理程的人員的角色及責任。定期就過去的事件進行趨勢分析，以助識別及防範類似問題。

(i) 變更管理

(i) 一般而言，變更管理是規劃、編排、應用、分配及記錄變更，以及對應用系統、系統軟件(例如操作系統及工具)、硬件、網絡系統及其他資訊科技設施及設備的變更進行實施後核實的程序。制定正式的變更管理程序，以確保作業環境的完整性及可靠性，變更是妥當的，以及對作業環境不會造成任何不利影響。此外，應建立管理緊急變更的正式程序(包括備存紀錄及認可安排)，以便能及時地在受控情況下應對意料之外的問題。

(j) 基本保安要求

(i) 有關管控程序及基本保安要求(包括操作系統、系統軟件、數據庫、伺服器及網絡裝置等的所有配置及設置)備有整全及準確的文件紀錄。定期檢討遵保安設置是否遵守基本要求。

<u>資訊科技服務的提供</u>

(k) 內部服務水平協議

(i) 資訊科技部門管理層與各業務單位訂立服務水平協議，內容涵蓋系統可用性及效能要求、容量增長及提供予用戶的支援水平等。由負責的資訊科技部門設立周全的程序，對提供議定的技術支援及服務作出管理。

(l) 系統可用性及容量管理

(i) 實施有效程序，確保系統可用性及表現持續得到監察，並及時和全面匯報例外情況。

(ii) 除作業環境外，容量規劃應延伸至備用系統及相關設施。

<u>資訊科技操作</u>

(m) 工作編排

(i) 最初的工作編排對已編排工作的更改應經適當授權，並有程序識別、調查及批准偏離標準工作編排的情況。

(n) 弱點及修補程式管理

(i) 運用自動化工具及人手方法，定期進行全面的弱點評估。就以互聯網為本的對外系統，弱點評估的範圍包括常見的互聯網弱點。

(ii) 制定修補程式管理程序，以涵蓋保安修補程式的識別、分類、優先次序及安裝。為能及時實施保安修補程式，每類保安修補程式的實施時限應按其重要程度及對系統的影響界定。

(o) 保安監察及匯報

(i) 實施保安監察工具，以：

- 按照持牌人界定的記錄保存政策保存系統、應用程式及網絡裝置的記錄，以便調查(如有需要)；

- 監察關鍵配置及保安設置，以識別對有關設置的未經授權變更，以及阻截資訊科技資產的異常情況，例如異常的用戶行為、異常的系統程序及記憶體存取及對裝置的惡意回調；
- 就關鍵系統及應用程序的保安記錄及事故進行即時分析，並迅速偵測任何潛在攻擊；以及
- 任何懷疑或已確認的違規情況必須交回事件處理組妥為處理、上報及舉報。

(p) 資訊科技設施及設備的保養

(i) 資訊科技設施及設備按照業內慣例及供應商建議的保養時間及規格維修保養，以確保有關設施及設備得到妥善支援。

(q) 流動資訊處理

(i) 若持牌人為其僱員提供流動裝置，應訂有涵蓋徵用、認證、強化、加密、數據備份及保存等範圍的政策及程序

(ii) 若持牌人正考慮採納自攜裝置的做法，應註明採納自攜裝置的範圍、可存取的資料及所存取的數據的保密性，並按照本《應用說明》所載的科技風險管理框架進行風險評估。

<u>網絡及基礎設施管理</u>

(r) 網絡管理

(i) 明確指派具備有關專門知識的人員負責網絡管理。網絡標準、設計、圖表及操作程序有正式文件記錄、保持更新、傳達予所有相關網絡員工及定期檢討。

(ii) 識別對持續提供網絡服務屬關鍵的通訊設施。一旦關鍵點或連結發生故障，自動經由其他路徑通訊，以將單點故障的情況減至最少。

(s) 網絡保安

(i) 建立安全的網絡基礎設施支援其系統。為防範與持牌人網絡的不安全連接，建立及實施有關使用網絡及網絡服務的程序。有關程序涵蓋：

- 可用的網絡及網絡服務；

- 決定哪些人士可連接特定網絡及網絡服務的授權程序；以及
- 保障連接網絡接駁點、網絡連接及網絡服務的管控措施及程序。

(ii) 考慮分隔內部網絡為不同網段，並計及每個網段所儲取的數據或所連接的系統。

(iii) 定期檢討路由器、防火牆及網絡伺服器等網絡裝置的保安參數設置，以確保有關設置仍然適用。備存及定期審視關鍵網絡裝置的每日活動的審計紀錄，並即時向網絡操作人員發出有關潛在違反保安事項的提示。

(iv) 妥善使用加密技術及網絡監察工具，涵蓋外部及內部網絡，以保障內部網絡、與第三方的通訊渠道及外部網絡內的敏感資料。

(t) 數據中心管理

(i) 就數據中心進行風險評估，以識別有關保安威脅及操作弱點，以及評估對數據中心的保障措施是否足夠。

(ii) 就實際進入持牌人的數據中心實施周全的保安管控，只按需要授給予進入數據中心的權利，並定期予以檢討。備存進入數據中心的記錄，並定期審視。若持牌人使用多租戶數據中心，應特別留意防範未經授權使用資訊科技設備的情況。

<u>資訊科技外判</u>

(u) 外判資訊科技至境外辦事處

(i) 若持牌人就某些資訊科技管控措施或支援活動的外判安排倚賴其境外辦事處(例如母公司、附屬公司、總辦事處或同集團的其他地區辦事處)或與其境外辦事處合作，本地及境外辦事處各自就有關範圍的責任在有關文件(例如政策、程序、外判及/或服務水平協議)清楚列明。

(v) 其他技術服務提供者的管理

(i) 除資訊科技外判外，持牌人可能會倚賴外部技術服務提供者提供技術相關支援及服務(例如電訊及網絡操作員)。制定有關如何管理不同類別的主要外部技術服務提供者的指引，包括服務提供者甄選程序、重大例外情況核准情況，以及需要避免過度倚賴單一技術服務提供者提供關鍵技術服務。

(w) 特別留意雲端資訊處理

(i) 雲端資訊處理普遍被視為資訊科技外判，持牌人若打算採用或已採用雲端資訊處理服務，應遵守有關指引文件，以及政府組織不時發出的任何有關指引或最佳做法。